PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-152194
(43)Date of publication of application : 24.05.2002

(51)Int.Cl. H04L 9/32
H04H 1/00
H04H 1/02
H04L 9/08
H04N 7/167

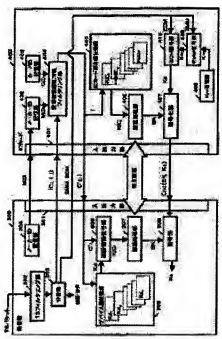
(21)Application number : 2000-344384
(22)Date of filing : 10.11.2000

(71)Applicant : TOSHIBA CORP
MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : OI SHINICHI
KUROIWA WATARU
KUMAZAKI HIROJI
SAIJO TAKESHI
INOUE TETSUYA
MATSUO TAKASHI
MURAKAMI HIRONORI
FUDA YUICHI
OMORI MOTOJI

(54) LIMITED RECEPTION DEVICE, LIMITED RECEPTION DEVICE AUTHENTICATING METHOD, AND CIPHER COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a limited reception device which actualizes mutual authentication of high reliability even if a reception device main body and a security module do not hold a common global secret.
SOLUTION: The reception device main body is equipped with a storage means which stores an ID for identifying a maker, a storage means which stores one or more pieces of information unique to the reception device main body, a deciphering means which deciphers information ciphered by using as a key the reception device main body unique information, and an authentication processing means which performs authentication processing with the security module by inputting the information outputted by the deciphering means. The security module is equipped with a storage means which stores a card ID for uniquely identifying the limited reception device, a means which filters reception device authentication information by referring to the maker ID and card ID, a storage means which stores one or more pieces of unique to the security module, and an authentication processing means which performs authentication processing with the reception device main body by inputting the security module unique information.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－152194
（P2002－152194A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.'	識別記号	F.I		テーマコード'（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｈ　1/00	Ｆ	５Ｃ０６４
Ｈ０４Ｈ　1/00		1/02	Ｅ	５Ｊ１０４
1/02		Ｈ０４Ｌ　9/00	６７５Ａ	
Ｈ０４Ｌ　9/08			６０１Ｃ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数27　ＯＬ　（全 22 頁）

(21)出願番号　特願2000－344384(P2000－344384)

(22)出願日　平成12年11月10日(2000.11.10)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

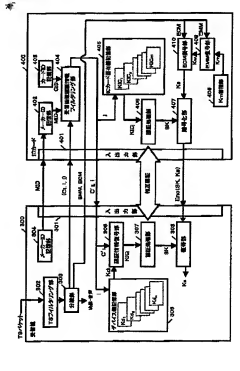
(72)発明者　大井　伸一
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内

(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　限定受信装置、限定受信装置認証方法及び暗号通信方法

(57)【要約】
【課題】　受信装置本体とセキュリティモジュールとが共通のグローバルシークレットを保持せずとも、信頼性が高い相互の認証を実現する限定受信装置を提供する。
【解決手段】　受信装置本体は、メーカーを識別するＩＤを記憶する記憶手段と、１つ以上の受信装置本体固有情報を記憶する記憶手段と、受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールは、限定受信装置を一意に識別するカードＩＤを記憶する記憶手段と、メーカーＩＤとカードＩＤとを参照して受信装置認証情報をフィルタリングする手段と、１つ以上のセキュリティモジュール固有情報を記憶する記憶手段と、セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行う認証処理手段を備える。



1

【特許請求の範囲】

【請求項１】　放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置の受信装置本体であって、

セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

１つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備することを特徴とする受信装置本体。

【請求項２】　前記メーカーＩＤを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段を具備することを特徴とする請求項１に記載の受信装置本体。

【請求項３】　放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置のセキュリティモジュールであって、

受信装置本体とのデータ入出力を行う入出力手段と、

限定受信装置を一意に識別するカードＩＤを記憶するカードＩＤ記憶手段と、

前記カードＩＤを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とするセキュリティモジュール。

【請求項４】　受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段をさらに具備し、

前記フィルタリング手段は、メーカーＩＤとカードＩＤとを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングすることを特徴とする請求項３に記載のセキュリティモジュール。

【請求項５】　前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項３及び請求項４のいずれか一項に記載のセキュリティモジュール。

2

【請求項６】　放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、

受信装置本体は、

セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

１つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、

セキュリティモジュールは、

受信装置本体とのデータ入出力を行う入出力手段と、

限定受信装置を一意に識別するカードＩＤを記憶するカードＩＤ記憶手段と、

受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

前記メーカーＩＤと前記カードＩＤとを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とする限定受信装置。

【請求項７】　前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項６に記載の限定受信装置。

【請求項８】　放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、

受信装置本体は、

セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

前記メーカーＩＤを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリン

グ手段と、
１つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、
前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、
前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、
セキュリティモジュールは、
受信装置本体とのデータ入出力を行う入出力手段と、
限定受信装置を一意に識別するカードＩＤを記憶するカードＩＤ記憶手段と、
前記カードＩＤを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、
１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、
前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とする限定受信装置。

【請求項９】　前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項８に記載の限定受信装置。

【請求項１０】　受信装置本体にセキュリティモジュールが装着されている限定受信装置の認証方法であって、
限定受信装置が、受信した放送波に含まれる受信装置認証情報を分離するステップと、
自受信装置宛の受信装置認証情報だけを取り出すフィルタリング処理ステップと、
受信装置本体が、前記受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成するステップと、
受信装置本体とセキュリティモジュールが、受信装置本体とセキュリティモジュールとが共有した前記セキュリティモジュール固有情報を用いて認証処理を行うステップを有することを特徴とする受信装置認証方法。

【請求項１１】　前記受信装置認証情報は、受信装置本体が１つ以上保持する受信装置本体固有情報のいずれか１つを鍵として、セキュリティモジュールが１つ以上保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報のいずれか１つを暗号化することにより生成される情報と、
受信装置本体のメーカーを識別するメーカーＩＤと、
受信装置を識別するカードＩＤとを含み、
受信装置認証情報の生成に用いた受信装置本体固有情報及びセキュリティモジュール固有情報を特定するためのインデックス情報に組み合わせて、放送局設備から放送波を用いて送出されることを特徴とする、請求項１０に記載の受信装置認証方法。

【請求項１２】　前記フィルタリング処理は、前記メーカーＩＤとセキュリティモジュールが記憶しているカードＩＤとが一致する受信装置認証情報を自受信装置宛の受信装置認証情報として選択することを特徴とする請求項１０及び請求項１１のいずれか一項に記載の受信装置認証方法。

【請求項１３】　受信装置本体で生成される前記共有情報は、前記受信装置本体固有情報を鍵として、前記受信装置認証情報に含まれる情報を復号することにより復元されることを特徴とする、請求項１０から請求項１２のいずれか一項に記載の受信装置認証方法。

【請求項１４】　前記フィルタリング処理は、受信装置本体において、受信装置本体が記憶しているメーカーＩＤと一致する受信装置認証情報を選択し、セキュリティモジュールにおいて、セキュリティモジュールが記憶しているカードＩＤと一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項１０から請求項１３のいずれか一項に記載の受信装置認証方法。

【請求項１５】　セキュリティモジュールは、セキュリティモジュールが受信装置本体に装着された後に受信装置本体から入力されるメーカーＩＤを記憶するステップを有することを特徴とする、請求項１０から請求項１３のいずれか一項に記載の受信装置認証方法。

【請求項１６】　前記フィルタリング処理は、セキュリティモジュールにおいて、前記記憶されたメーカーＩＤとセキュリティモジュールが記憶しているカードＩＤとが一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項１５に記載の受信装置認証方法。

【請求項１７】　セキュリティモジュールは、フィルタリング処理により抽出した受信装置認証情報を記憶するステップを有し、セキュリティモジュールが受信装置本体に装着された後に受信装置本体から入力されるメーカーＩＤが前記記憶している受信装置認証情報に含まれるメーカーＩＤと等しい場合は、前記記憶している受信装置認証情報を受信装置本体に出力し、受信装置本体は、セキュリティモジュールから渡された前記受信装置認証情報を基に前記共有情報を生成することを特徴とする、請求項１４から請求項１６のいずれか一項に記載の受信装置認証方法。

【請求項１８】　認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と、
乱数を出力する乱数生成手段と、
前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、
前記暗号鍵を用いてセキュリティモジュールから入力される情報を復号する復号手段とをさらに具備することを特徴とする、請求項１及び請求項２のいずれか一項に記

載の受信装置本体。

【請求項１９】　前記暗号鍵を用いてセキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備することを特徴とする、請求項１８に記載の受信装置本体。

【請求項２０】　認証処理手段が出力した受信装置本体との共有値を記憶する記憶手段と、

前記記憶している共有値と受信装置本体から入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて受信装置本体へ出力する情報を暗号化する暗号化手段とをさらに具備することを特徴とする、請求項３から請求項５のいずれか一項に記載のセキュリティモジュール。

【請求項２１】　前記暗号鍵を用いて受信装置本体から入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項２０に記載のセキュリティモジュール。

【請求項２２】　放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、

受信装置本体は、

セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

１つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段と、

前記認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と、

乱数を出力する乱数生成手段と、

前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いてセキュリティモジュールから入力される情報を復号する復号手段とを具備し、

セキュリティモジュールは、

受信装置本体とのデータ入出力を行う入出力手段と、

限定受信装置を一意に識別するカードＩＤを記憶するカードＩＤ記憶手段と、

受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

前記メーカーＩＤと前記カードＩＤとを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段と、

前記認証処理手段が出力した受信装置本体との共有値を記憶する記憶手段と、

前記記憶している共有値と受信装置本体から入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて受信装置本体へ出力する情報を暗号化する暗号化手段とを具備することを特徴とする限定受信装置。

【請求項２３】　前記受信装置本体は、

前記暗号鍵を用いてセキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備し、

前記セキュリティモジュールは、

前記暗号鍵を用いて受信装置本体から入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項２２に記載の限定受信装置。

【請求項２４】　受信装置本体にセキュリティモジュールが装着されている限定受信装置の受信装置本体とセキュリティモジュール間の暗号通信方法であって、

受信装置本体は、セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップを有し、

セキュリティモジュールは、受信装置本体との認証処理によって生成した共有値を記憶するステップを有し、

受信装置本体及びセキュリティモジュールは、それぞれが記憶した共有値を鍵として用いて暗号通信を行うことを特徴とする、暗号通信方法。

【請求項２５】　受信装置本体にセキュリティモジュールが装着されている限定受信装置の受信装置本体とセキュリティモジュール間の暗号通信方法であって、

受信装置本体は、

セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップと、

乱数を生成するステップと、

前記乱数をセキュリティモジュールに出力するステップと、

前記記憶したセキュリティモジュールとの共有値と前記乱数とを用いて暗号鍵を生成するステップとを有し、

セキュリティモジュールは、

受信装置本体との認証処理によって生成した共有値を記憶するステップと、

前記記憶した受信装置本体との共有値と受信装置本体から入力された乱数とを用いて暗号鍵を生成するステップと、

前記暗号鍵を受信装置本体との共有値として記憶するス

テップとを有し、
受信装置本体及びセキュリティモジュールは、それぞれが生成した暗号鍵を用いて暗号通信を行うことを特徴とする、暗号通信方法。

【請求項２６】　受信装置本体は、前記生成した暗号鍵をセキュリティモジュールとの新しい共有値として記憶するステップをさらに有し、
セキュリティモジュールは、前記生成した暗号鍵を受信装置本体との新しい共有値として記憶するステップをさらに有することを特徴とする、請求項２５に記載の暗号通信方法。

【請求項２７】　受信装置本体からセキュリティモジュールへのコマンド送信をトリガーとして、受信装置本体が前記乱数を生成することを特徴とする、請求項２５及び請求項２６のいずれか一項に記載の暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、視聴契約を必要とする放送システム（限定受信システム）の限定受信装置に関し、特に、受信装置本体にセキュリティモジュールが装着される限定受信装置、限定受信装置の認証方法、及び暗号通信方法に関する。

【０００２】

【従来の技術】従来の標準的な限定受信方法であるＭＰＥＧ２ＳＹＳＴＥＭＳ（ＩＳＯ／ＩＥＣ１３８１８－１）では、送出側は、映像や音声等のコンテンツをスクランブル鍵Ｋｓでスクランブルして送信し、また、このスクランブル鍵ＫｓをＥＣＭ（Entitlement Control Messages：番組情報）に格納した後、このＥＣＭをワーク鍵Ｋｗで暗号化して送信する。また、ワーク鍵Ｋｗは、事前にＥＭＭ（Entitlement Management Messages：個別情報）に格納され、個別鍵Ｋｍで暗号化されて送信される。

【０００３】図１は、この送出側の構成を示している。映像や音声等のコンテンツを生成するコンテンツ生成部１００と、Ｋｓを生成するＫｓ生成部１０１と、コンテンツをＫｓでスクランブルするスクランブラ１０６と、Ｋｓを格納したＥＣＭを生成するＥＣＭ生成部１０２と、Ｋｗを生成するＫｗ生成部１０３と、Ｋｗを用いてＥＣＭを暗号化するＥＣＭ暗号化部１０７と、Ｋｗを格納したＥＭＭを生成するＥＭＭ生成部１０４と、Ｋｍを生成するＫｍ生成部１０５と、Ｋｍを用いてＥＭＭを暗号化するＥＭＭ暗号化部１０８と、スクランブルされたコンテンツや暗号化されたＥＣＭ及びＥＭＭを多重化する多重化部１０９とを備えている。

【０００４】ＥＣＭには、Ｋｓの他に、番組識別情報である番組ティア情報や現在時刻が格納され、これらがＫｗで暗号化される。また、ＥＣＭには、非暗号のモジュール識別フラグが付される。また、ＥＭＭには、Ｋｗの他に、該当する受信装置の視聴権を識別するための個別ティア情報や視聴契約の情報が格納され、これらがＫｍで暗号化される。また、ＥＭＭには、非暗号のモジュール識別フラグ及び該当する受信装置のＩＤが付される。

【０００５】多重化部で多重化された信号はＴＳパケット（Transport Stream Packet）に変換されて送出される。一方、番組を視聴する受信側の構成は、図２に示すように、受信装置本体（受信機）１１０と、受信機に装着されるＩＣカード等のセキュリティモジュール１２０とを備えており、受信機は選局されたＴＳパケットだけを取り込むＴＳフィルタリング部１１１と、多重されている信号を分離する分離部１１２と、スクランブルされたコンテンツを復号化するデスクランブラ１１３とを具備し、また、セキュリティモジュールは、Ｋｍを保持するＫｍ蓄積部１２１と、Ｋｍを用いてＥＭＭを復号するＥＭＭ復号部１２２と、Ｋｗを用いてＥＣＭを復号するＥＣＭ復号部１２３とを具備している。

【０００６】受信機は、自己宛のＥＭＭが送られてくるとこれを受信する。ＥＭＭは、視聴契約の更新等に伴って送られて来る。このＥＭＭは、分離部１１２で分離されてＥＭＭ復号部１２２に出力され、ＥＭＭ復号部は、Ｋｍ蓄積部１２１に蓄積されているＫｍを用いてこれを復号し、ＥＭＭに含まれるＫｗ，個別ティア情報及び契約情報などをＥＣＭ復号部１２３に出力する。ＥＣＭ復号部は、これらの情報を保持する。

【０００７】受信機が、スクランブルされたコンテンツと、そのスクランブル鍵Ｋｓを含むＥＣＭとを受信すると、スクランブルされたコンテンツは、分離部１１２で分離されてデスクランブラ１１３に送られ、また、分離されたＥＣＭはＥＣＭ復号部１２３に送られる。ＥＣＭ復号部は、このＥＣＭを、前記保持したＫｗで復号化し、そこに含まれた現在時刻を視聴契約の有効期間と比較し、また、番組ティア情報を個別ティア情報と比較して、チャンネル視聴権の有無を識別する。そして、チャンネル視聴権が認められる場合にだけ、復号したＫｓを受信機のデスクランブラ１１３に出力する。受信機のデスクランブラは、セキュリティモジュールから送られてくるＫｓを順次取得し、コンテンツのスクランブルを解く。こうしてスクランブルされた番組の視聴が可能になる。

【０００８】しかし、この場合、セキュリティモジュールから受信機に非暗号の状態のＫｓが渡されるため、その通信路上でＫｓが不正に取得され、視聴契約をしていない者がコンテンツのデスクランブルにＫｓを不正利用する恐れがある。特開平０９－４６６７２号公報には、こうした点を改善するため、セキュリティモジュールと受信機とが共通鍵を保持し、セキュリティモジュールはＫｓを共通鍵で暗号化して受信機に送り、受信機はこれを共通鍵で復号してＫｓを取り出す方式が記載されている。この場合、共通鍵がセキュリティモジュールから受信機へ渡される際に不正に取得される恐れがあり、この

共通鍵が不正に取得されると、結局、Ｋｓが不正に取得されてしまう。

【０００９】特開平０２－１９５３７６号公報には、ＩＣカード間での安全な鍵共有方法が記載されている。それによると、第２のＩＣカードが乱数を生成し、その乱数をマスタ鍵で暗号化して第１のＩＣカードに渡し、第１のＩＣカードは前記の暗号化された乱数をマスタ鍵で復号して乱数を復元し、第１のＩＣカードと第２のＩＣカードは共有した前記乱数をセッション鍵として暗号通信を行う。この場合、第１のＩＣカードと第２のＩＣカードは予めグローバルシークレットであるマスタ鍵を共有しているので、乱数を安全に共有することが可能である。

【００１０】

【発明が解決しようとする課題】これまでの説明から明らかなように、受信装置本体とセキュリティモジュールとの間で安全な暗号通信を行うためには、受信装置本体とセキュリティモジュールとが、共有情報を安全に共有することが重要である。予め共有情報をグローバルシークレットとして受信装置本体とセキュリティモジュールとに格納した場合、セッション毎に相互認証を行うことにより、セッション毎に異なる安全なセッション鍵を共有することが可能である。しかし、この場合、悪意を持つ者が受信装置装置とセキュリティモジュールとの間で通信される相互認証用データ（チャレンジ・レスポンス等）を不正取得して暗号解読を試み、万が一、共有情報の割り出しに成功すると、セッション鍵の割り出しが可能となり、その結果、スクランブル鍵Ｋｓや、視聴契約情報、課金情報といった受信装置本体とセキュリティモジュールとの間で通信されるデータが不正に取得されてしまう。また、割り出された共有情報は、全ての受信装置において共通であるため、限定受信システム運用に与えるダメージは非常に重大である。システム運用を回復するための対処として、新しい共有情報を暗号化して格納した記憶メディアを全視聴者に配布して受信機及びセキュリティモジュールの共有情報を更新する方法が考えられるが、これは膨大なコストの発生を伴うと予想され、非現実的である。

【００１１】また、受信装置本体とＩＣカード等のセキュリティモジュールの製造は、それぞれ複数の異なるメーカーが担当するのが一般的である。予め共有情報を受信装置本体及びセキュリティモジュールに格納しておく場合、全てのメーカー製の受信装置本体と、全てのメーカー製のセキュリティモジュールとの組み合わせにおいて相互認証を正しく行うためには、メーカーを問わず、全ての受信機及びセキュリティモジュールで等しい共有情報を共有する必要がある。この場合、ある１つのメーカーにおける機密情報管理レベルが低く、メーカー内部から共有情報の漏洩が発生してしまうと、他のメーカー製の受信装置本体及びセキュリティモジュールにもその影響が波及し、限定受信システムの運用に致命的なダメージを及ぼすことになる。

【００１２】本発明は、こうした問題点を解決するものであり、受信装置本体とセキュリティモジュールとで予め共通の共有情報を持たずとも、セッション鍵生成等で用いる共有情報を安全に共有することができる限定受信装置の認証方法、及び、限定受信装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】この課題を解決するために本発明は、受信装置本体にセキュリティモジュールが装着される構成を取る限定受信装置において、受信装置本体は受信装置本体を製造するメーカーを識別するＩＤを記憶するメーカーＩＤ記憶手段と、１つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールは限定受信装置を一意に識別するカードＩＤを記憶するカードＩＤ記憶手段と、メーカーＩＤとカードＩＤとを参照して受信装置認証情報をフィルタリングするフィルタリング手段と、１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行う認証処理手段を備えることを特徴とする。

【００１４】また、放送局設備において受信装置認証情報を生成し、受信装置認証情報を放送局から放送波を用いて送出し、限定受信装置は受信した受信装置認証情報からメーカーＩＤとカードＩＤを検索キーとして自受信装置宛の受信装置認証情報だけをフィルタリングし、受信装置本体はフィルタリングした受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成して、受信装置本体とセキュリティモジュールは前記共有情報を用いて認証処理を行う。

【００１５】また、受信装置認証情報は、受信装置本体が保持する受信装置本体固有情報を鍵としてセキュリティモジュールが保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報を暗号化することにより生成される情報と、受信装置本体のメーカーを識別するメーカーＩＤと、受信装置を識別するカードＩＤとから構成する。

【００１６】以上により、受信装置本体とセキュリティモジュールとでセキュリティモジュール固有情報を共有し、その共有情報を基に、受信装置本体とセキュリティモジュールとの間の暗号通信に用いるセッション鍵を生成する。また、受信装置本体は乱数生成手段と、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備え、セキュリティモジュールは、セッショ

ン鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備える。

【００１７】また、受信装置本体は乱数を生成してセキュリティモジュールに出力すると共に、セッション鍵記憶手段から読み出したセッション鍵と前記乱数とから暗号鍵を生成する。さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。セキュリティモジュールは、受信装置本体から入力した乱数と、セッション鍵記憶手段から読み出したセッション鍵とから暗号鍵を生成する、さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。

【００１８】以上により、受信装置本体とセキュリティモジュールとで共通の暗号鍵を共有し、暗号通信を行う。

【００１９】

【発明の実施の形態】本発明の実施の形態について、図を用いて説明する。なお、以降では、受信装置本体を受信機、セキュリティモジュールをＩＣカード、受信装置本体固有情報をデバイス鍵、セキュリティモジュール固有情報をＩＣカード固有鍵と記述して説明する。

【００２０】図３は、放送局で管理するデバイス鍵及びＩＣカード固有鍵をそれぞれ受信機及びＩＣカードに格納する手順の一例を示す図である。放送局２００の一設備である鍵管理センタ２０１は、受信機メーカー毎に固有のｎ個のデバイス鍵Kd_i（$1 \leq i \leq n$）を生成する。ここで、ｉはデバイス鍵のインデックス番号である。ｎの値については後述する。

【００２１】デバイス鍵の値は受信機メーカー毎に異なる。同一のメーカーが製造する全ての受信機には同じ値のデバイス鍵$Kd_1 \sim Kd_n$が格納される。デバイス鍵生成部２０２で生成された各デバイス鍵は、鍵管理センタ内のデバイス鍵ＤＢ２０３に受信機メーカーを識別するメーカーＩＤと共に登録され、安全に管理される。例えば、第３者の立ち入りが制限された機密情報管理室にて管理される。

【００２２】受信機メーカー２０６は、放送局から安全な手段により配送される自メーカー用のデバイス鍵を受け取り、デバイス鍵を受信機２０７の製造時に受信機内部のデバイス鍵記憶部に格納する。放送局から受信機メーカーへのデバイス鍵配送は、例えば、ＣＤ－ＲＯＭのような記録メディアに暗号化したデバイス鍵を記録し、オフライン配送する。

【００２３】１つの受信機にはｎ個のデバイス鍵が格納される。なお、受信機内部のデバイス鍵記憶部をデータの取り出しが困難なＬＳＩ内部等に具備することにより、悪意ある受信機ユーザによるデバイス鍵暴露の可能性を低くすることができる。また一方、鍵管理センタは、ＩＣカード毎に固有のｍ個のＩＣカード固有鍵KIC_j（$1 \leq j \leq m$）を生成する。ここで、ｊはＩＣカード固有鍵のインデックス番号である。ｎ及びｍの値は、セキュリティ的観点や受信機及びＩＣカードの配憶容量等から限定受信システム仕様として規定される。ｎ及びｍの値が大きいほどセキュリティ度は高まるが、受信機及びＩＣカードの記憶容量が多く必要となるため、コスト的に不利となる。

【００２４】ＩＣカード固有鍵の値は、ＩＣカードメーカーの区別なく、製造発行される全てのＩＣカード毎に異なる。ＩＣカード固有鍵生成部２０４で生成された各ＩＣカード固有鍵は、鍵管理センタ内のＩＣカード固有鍵ＤＢ２０５にＩＣカードを識別するカードＩＤと共に登録され、デバイス鍵と同様に安全に管理される。なお、ＩＣカード固有鍵の値は、製造ロット単位で異なるとしても構わない。

【００２５】ＩＣカードメーカー２０８は、放送局から安全な手段により配送されるＩＣカード固有鍵を受け取り、ＩＣカード固有鍵をＩＣカード製造時にＩＣカード内部のＩＣカード固有鍵記憶部に格納する。一般にＩＣカードは耐タンパ性を有しており、ＩＣカード内のＩＣカード固有鍵記憶部への外部からのアクセスは困難であり、ＩＣカードからＩＣカード固有鍵が暴露される可能性は低い。

【００２６】なお、図３ではデバイス鍵を放送局側にて生成して、受信機メーカーに配布する形態となっているが、各受信機メーカーが自メーカーのデバイス鍵を生成し、放送局の鍵管理センタに登録する形態としても構わない。また、図３では鍵管理センタが放送局内の一設備とする構成になっているが、放送局とは独立した構成となっていてもよい。

【００２７】図４は、受信装置認証情報を生成する方法を示す図である。鍵管理センタ２０１の受信装置認証情報生成部２１０には、デバイス鍵ＤＢ２０３からデバイス鍵及びメーカーＩＤ、ＩＣカード固有鍵ＤＢ２０５からＩＣカード固有鍵及びカードＩＤが入力される。暗号化部２１１は、ＩＣカード固有鍵KIC_jに対しデバイス鍵Kd_iを鍵として共通鍵暗号で暗号化した$Enc(Kd_i, KIC_j)$を生成して出力する。ここで、$Enc(X, Y)$は、データＹを鍵Ｘで暗号化した暗号化データを表わす。さらに、暗号化部が出力した前記暗号化データにメーカーＩＤとＩＣカードＩＤを付加することにより、受信装置認証情報$C_{ij} = Enc(Kd_i, KIC_j) | MID | CID$となる。ここでＸ｜Ｙは、データＸとデータＹを結合したデータを表わす。ある一つの受信機メーカーが製造する受信機と、一つのＩＣカードとの組み合わせに対する受信装置認証情報は、$C_{i1}, C_{i2}, \ldots, C_{in}, C_{j1}, C_{j2}, \ldots, C_{jn}$の合計ｎ×ｍ個が生成される。

【００２８】図５は、放送波を用いて受信装置認証情報を受信装置側へ送出する、送信側のブロック図である。(C_{ij}, i, j)生成部１３０では受信装置確認情報Ｃ

$_{ij}$とそのインデックス情報ｉ及びｊとを組み合わせたしたデータ（C_{ij}，ｉ，ｊ）を生成する。そして、スクランブル鍵Ｋｓでスクランブルされたコンテンツに個別鍵ＫｍでＭＭＩとワーク鍵Ｋｗで暗号化したＥＭＭを多重化するのと同様に、多重化部１３１において（C_{ij}，ｉ，ｊ）をコンテンツ等と多重化し、その信号をＴＳパケットに変換し放送波として送出する。なお、（C_{ij}，ｉ，ｊ）をＥＣＭやＥＭＭに格納して放送波として送出する形態であっても構わない。

【００２９】図６は、受信した受信装置認証情報を用いて受信装置とＩＣカードとの間でＩＣカード固有鍵を共有し、共有したＩＣカード固有鍵を用いて相互認証を実行してセッション鍵を共有してスクランブル鍵Ｋｓを暗号通信する方法を説明するブロック図である。まず、ＩＣカードＡ４００は、受信機３００に接続された際の初期処理において、受信機がメーカーＩＤ記憶部３０４に記憶している受信機のメーカーＩＤ（ＭＩＤ）を受け取り、メーカーＩＤ記憶部４０２にＭＩＤを記憶する。受信機が受信した放送波（ＴＳパケット）は、分離部３０３において、映像・音声信号、ＥＭＭ、ＥＣＭ、（C_{ij}，ｉ，ｊ）に分離される。受信機は、放送波に含まれる全ての（C_{ij}，ｉ，ｊ）を入出力部３０１からＩＣカードに送信し、ＩＣカードでは、入出力部４０１において受信した（C_{ij}，ｉ，ｊ）を受信装置認証情報フィルタリング部４０４に入力する。受信装置認証情報フィルタリング部では、メーカーＩＤ記憶部４０２に記憶されたＭＩＤとカードＩＤ記憶部４０３に記憶されているＣＩＤとを参照して、全ての（C_{ij}，ｉ，ｊ）のうちからＭＩＤとＣＩＤの両方が一致するC_{ij}（＝Ｅｎｃ（K_{di}，ＫＩＣ$_j$）｜ＭＩＤ｜ＣＩＤ）、ｉ及びｊの組み合わせを抽出する。ＭＩＤまたはＣＩＤが一致しない（C_{ij}，ｉ，ｊ）は破棄する。ＩＣカードは、抽出したC_{ij}からＭＩＤとＣＩＤとを取り除いたC'_{ij}（＝Ｅｎｃ（K_{di}，ＫＩＣ$_j$））とｉとを入出力部４０１から受信機に送信する。また、ｊの値に対応するＩＣカード固有鍵ＫＩＣ$_j$をＩＣカード固有鍵記憶部４０５から読み出す。

【００３０】受信機はＩＣカードからC'_{ij}及びｉを受信すると、まずｉの値に対応するデバイス鍵K_{di}をデバイス鍵記憶部３０５から読み出す。次に、認証情報復号部３０６において、K_{di}を鍵としてC'_{ij}を復号し、ＩＣカード固有鍵ＫＩＣ$_j$を得る。ここで、受信機の認証情報復号部で用いられる暗号アルゴリズムは、放送局の鍵管理センタで受信装置認証情報を生成した際に用いた共通鍵暗号アルゴリズムに等しい。なお、前記暗号アルゴリズムは、公開鍵暗号アルゴリズムであってもよい。

【００３１】このように、受信機とＩＣカードにおいて、予め共有した情報を持たない状態からＩＣカード固有鍵ＫＩＣ$_j$を安全に共有することが可能である。さらに、受信機の認証処理部３０７とＩＣカードの認証処理部４０６は、前記共有したＩＣカード固有鍵ＫＩＣ$_j$を用いた相互認証を実行し、セッション鍵ＳＫを生成して共有する。ＩＣカードは、受信機からＥＭＭを受け取るとＥＭＭ復号部４０９でＫｍ蓄積部４０８に記憶している個別鍵ＫｍでＥＭＭを復号して得たワーク鍵ＫｗをＥＣＭ復号部に出力し、また、受信機からＥＣＭを受け取るとＥＣＭ復号部４１０で前記Ｋｗを用いてＥＣＭを復号してスクランブル鍵Ｋｓを得る。ＩＣカードの暗号化部４０７は前記ＳＫを暗号化鍵としてＫｓを暗号化したＥｎｃ（ＳＫ，Ｋｓ）を受信機に出力する。受信機の復号部３０８は前記ＳＫを復号鍵として、ＩＣカードから受信した前記Ｅｎｃ（ＳＫ，Ｋｓ）を復号し、スクランブル鍵Ｋｓを出力する。

【００３２】このように、認証処理の度に更新されるセッション鍵ＳＫを用いた暗号通信が可能なため、スクランブル鍵ＫｓをＩＣカードから受信機へ高いセキュリティを維持して送信することができる。図７は、受信機とＩＣカードとのチャレンジ・レスポンスによる相互認証フローの一例を示す図である。以下の説明において、受信機側処理は受信機３００の相互認証部３１０で、ＩＣカード側の処理はＩＣカードＡ４００の相互認証部４１３で行われる。受信機は乱数Ｒ１を生成してＩＣカードに送信する。また、受信機はＫＩＣ$_j$を鍵としてＲ１を暗号化し、Ｅｎｃ（ＫＩＣ$_j$，Ｒ１）を生成する。ＩＣカードはＲ１を受信すると、ＫＩＣ$_j$を鍵としてＲ１を暗号化し、Ｅｎｃ（ＫＩＣ$_j$，Ｒ１）を生成する。さらに乱数Ｒ２を生成して、Ｅｎｃ（ＫＩＣ$_j$，Ｒ１）及びＲ２を受信機に送信する。また、ＩＣカードはＫＩＣ$_j$を鍵としてＲ２を暗号化し、Ｅｎｃ（ＫＩＣ$_j$，Ｒ２）を生成する。受信機は、ＩＣカードからＥｎｃ（ＫＩＣ$_j$，Ｒ１）及びＲ２を受信すると、既に受信機にて作成済みのＥｎｃ（ＫＩＣ$_j$，Ｒ１）とＩＣカードから受信したＥｎｃ（ＫＩＣ$_j$，Ｒ１）を比較して、値が一致することを確認する。前記Ｅｎｃ（ＫＩＣ$_j$，Ｒ１）の値が一致した場合、ＫＩＣ$_j$を鍵としてＩＣカードから受信したＲ２を暗号化してＥｎｃ（ＫＩＣ$_j$，Ｒ２）を生成し、ＩＣカードへ送信する。ＩＣカードは、受信機からＥｎｃ（ＫＩＣ$_j$，Ｒ２）を受信すると、既にＩＣカードにて作成済みのＥｎｃ（ＫＩＣ$_j$，Ｒ２）とＩＣカードから受信したＥｎｃ（ＫＩＣ$_j$，Ｒ２）を比較して、値が一致することを確認する。そして、受信機とＩＣカードはそれぞれ、Ｒ１とＲ２を合成したＲ１・Ｒ２に対し、ＫＩＣ$_j$を鍵として暗号化することにより、セッション鍵ＳＫを得る。ここで、受信機とＩＣカードそれぞれの相互認証部が備える暗号アルゴリズムは等しい。

【００３３】なお、上記チャレンジ・レスポンスによる相互認証フローは一例に過ぎず、ＫＩＣ$_j$を共有秘密情報として用い、その他の相互認証方式を適用してセッシ

ョン鍵ＳＫを共有してもよい。また、受信機またはＩＣカードの片方向認証であってもよい。また、セッション鍵ＳＫは、受信機の電源投入時、受信機へのＩＣカード挿入時などのタイミングで、相互認証し共有するものであるが、相互認証において、受信機およびＩＣカードが個々に生成している乱数が相互認証を行う都度異なることがセキュリティ上重要である。すなわち、受信機がＩＣカードを認証する場合を考えると、上記タイミングで生成する乱数Ｒｉが、その都度異なる乱数であれば、以前の相互認証に使用したものと同じＫＩＣｊをもし使用する場合であっても、Ｅｎｃ（ＫＩＣｊ、Ｒ１）は異なるデータとなり、不正なＩＣカードが、正規ＩＣカードが相互認証に使用した過去のデータを流用してなりすまそうとしても不可能であり、なりすましの不正を防止することが可能となる。同様にＩＣカードが受信機を認証する場合にも、乱数Ｒ２が、その都度異なる乱数であれば、以前の相互認証に使用したものと同じＫＩＣｊを使用する場合であっても、Ｅｎｃ（ＫＩＣｊ、Ｒ２）は異なるデータとなり、不正な受信機が、正規受信機が相互認証に使用した過去のデータを流用して、なりすまそうとしても不可能であり、なりすましの不正を防止することが可能となる。

【００３４】以上説明した、相互認証の際に同じ乱数が生成されないようにするための方法として、不揮発メモリ回路の利用がある。すなわち、乱数生成器が、生成した状態を不揮発メモリに記憶しておき、次回生成する乱数はその状態から継続生成することで同じ乱数の生成を防ぐものである。あるいは、乱数生成器が、初期化データを与え、乱数を得る構成とし、今回生成した乱数を記憶しておき、次回の初期化データとすることにより同じ乱数の生成を防ぐものである。

【００３５】図８は、図６で説明した構成において、ＩＣカード４００に受信装置認証情報記憶部４１１を備えた場合を示す図である。ＩＣカードの受信装置認証情報フィルタリング部４０４では、メーカーＩＤ記憶部４０２に記憶されているＭＩＤとカードＩＤ記憶部４０３に記憶されているＣＩＤとを参照して、全ての（C_{ij}，ｉ，ｊ）のうちからＭＩＤとＣＩＤが一致するC_{ij}、ｉ及びｊの組み合わせを抽出する。ＭＩＤまたはＣＩＤが一致しない（C_{ij}，ｉ，ｊ）は破棄する。そして、抽出したC_{ij}からＭＩＤとＣＩＤとを取り除いたC'_{ij}及びｉを受信機に送信するとともに、送信したC'_{ij}とｉ、ｊ、及び前記抽出したC_{ij}に含まれていたＭＩＤを受信装置認証情報記憶部４１１に記憶する。

【００３６】図９は、ＩＣカードが受信機に装着された後に認証処理に至るまでの処理フローを示す図である。ＩＣカードの処理フローにおいて、受信装置認証情報記憶部を備えていない場合のフローを実線矢印で、受信装置認証情報記憶部を備えている場合のフローを破線矢印で記述している。受信機においては、ＩＣカードに受信装置認証情報記憶部を備えている場合と、備えていない場合とで処理フローに違いはない。受信機は、ＩＣカードが装着されると、ＭＩＤをＩＣカードに送信する（ステップＳ１００）。そして、放送波に含まれる（C_{ij}，ｉ，ｊ）を検出すると、ＩＣカードに送信する（ステップＳ１０１）。その後、ＩＣカードからC'_{ij}，ｉが入力されると、デバイス鍵記憶部からデバイス鍵K_{di}を読み出し、K_{di}を鍵としてC'_{ij}を復号してＫＩC_jを得て（ステップＳ１０３）、そのＫＩC_jを用いてＩＣカードとの認証処理を実行する（ステップＳ１０４）。

【００３７】一方、ＩＣカードにおいては、受信装置認証情報記憶部を備えている場合と、備えていない場合とで処理フローが異なる。まず、ＩＣカードに受信装置認証情報記憶部を備えていない場合のフローを説明する。ＩＣカードは、受信機からＭＩＤを受け取り、メーカーＩＤ記憶部に記憶する（ステップＳ１１０）。そして、受信機から（C_{ij}，ｉ，ｊ）が入力されるのを待つ（ステップＳ１１１）。（C_{ij}，ｉ，ｊ）が入力されると、ＭＩＤとＣＩＤの一致するC_{ij}を抽出してC'_{ij}を作成し（ステップＳ１１２）、C'_{ij}とｉを受信機に出力する（ステップＳ１１３）。さらに、ＩＣカード固有鍵記憶部から前記ｊに対応するKIC_jを読み出し（ステップＳ１１４）、そのKIC_jを用いて受信機との認証処理を実行する（ステップＳ１１５）。

【００３８】次に、ＩＣカードに受信装置認証情報記憶部を備えている場合のフローを説明する。ＩＣカードは、受信機からＭＩＤを受け取ると、メーカーＩＤ記憶部にＭＩＤを記憶する（ステップＳ１１０）。そして、受信装置認証情報記憶部からC'_{ij}、ｉ、ｊ、及びＭＩＤの読み出しを試みる（ステップＳ１２０）。受信装置認証情報記憶部にC'_{ij}、ｉ、ｊ、及びＭＩＤが記憶されていて、読み出しに成功した場合は、受信機から受け取った前記ＭＩＤと比較する（ステップＳ１２１）。ＭＩＤが等しい場合、受信装置認証情報記憶部から読み出したC'_{ij}とｉを受信機に出力する（ステップＳ１１３）。ステップＳ１２０において受信装置認証情報記憶部にC'_{ij}、ｉ、ｊ、及びＭＩＤが記憶されていない場合、または、ステップＳ１２１において前記ＭＩＤの比較結果が等しくない場合は、受信機から（C_{ij}，ｉ，ｊ）が入力されるのを待って（ステップＳ１１１）、フィルタリング処理によりC'_{ij}を作成する（ステップＳ１１２）。そして、C'_{ij}、ｉ、ｊ、及びＭＩＤを受信装置認証情報記憶部に記憶した後（ステップＳ１２２）、C'_{ij}とｉを受信機に出力する（ステップＳ１１３）。その後は、受信装置認証情報記憶部を備えている場合と同様である。

【００３９】このように、ＩＣカードに受信装置認証情報記憶部を備えて、受信機に送信したC'_{ij}、ｉ、ｊ、及び受信機のＭＩＤを記憶しておくと、次回以降にＩＣカードを装着した際に受信機のメーカーが前回と同じ場

合、受信機からの受信装置認証情報受信を待つことなく、すみやかに受信機との相互認証を開始することができる。

【００４０】図１０は、図６で説明した構成において、受信機３００にも受信装置認証情報フィルタリング部３０９を備えた場合を示す図である。受信機の受信装置認証情報フィルタリング部３０９は、分離部３０３によって分離された（C_U，ｉ，ｊ）のうちから、ＭＩＤが一致しないC_Uを破棄し、メーカーＩＤが一致したC_Uとｉ及びｊの組み合わせだけをＩＣカードに送信する。ＩＣカードの受信装置認証情報フィルタリング部４１２は、受信した（C_U，ｉ，ｊ）のうちからＣＩＤが一致するC_Uとｉ及びｊの組み合わせだけを抽出し、ＣＩＤが一致しないC_Uは破棄する。

【００４１】このように、受信機にも受信装置認証情報フィルタリング部を備えた場合、ＩＣカードに送信する（C_U，ｉ，ｊ）の数を削減することができ、ＩＣカードの受信装置認証情報フィルタリング部での処理量を削減することができるため、ＩＣカードの処理負荷を低減することが可能である。一般に、ＩＣカードと比較して受信機は処理能力が高いので、受信装置認証情報フィルタリング部を備えても大きな負荷増とはならない。また、ＩＣカードにメーカーＩＤ記憶部が不必要となる利点がある。

【００４２】図１１は、受信機とＩＣカードが暗号通信する方法を説明するブロック図である。まず、受信機がＩＣカードに対してコマンドを送信し、そのレスポンスとしてＩＣカードからの暗号化された通信データを受信機が受信する処理について説明する。たとえば、受信機がＥＣＭを受信した場合、受信機はＥＣＭ受信コマンドをＩＣカードにＥＣＭと共に送信し、そのレスポンスとして暗号化されたスクランブル鍵Ｋｓを受信する。

【００４３】受信機及びＩＣカードは、ＩＣカード固有鍵K_{IC}を基に相互認証処理を行って、それぞれセッション鍵ＳＫを保持する。受信機はＳＫ記憶部３２０に、ＩＣカードはＳＫ記憶部４２０にＳＫを記憶する。受信機の乱数生成部３２１は、乱数Ｒを生成する。コマンド生成部３２２は、ユーザによる操作や、放送波受信をトリガーとしてＩＣカードへのコマンドを生成する。その際、前記乱数ＲをコマンドデータのⅠ部として構成し、コマンドＣＯＭ（Ｒ）をＩＣカードに送信する。ここでＣＯＭ（Ｘ）は、データＸを含んだコマンドデータを示す。また、受信機の暗号鍵生成部３２３は、ＳＫ記憶部に記憶されているセッション鍵ＳＫと前記乱数Ｒを入力として暗号鍵ＳＫ’を生成し、復号部３０８に出力する。さらに、暗号鍵生成部３２３は前記生成したＳＫ’をＳＫ記憶部３２０に出力し、ＳＫを更新する。復号部３０８は、ＩＣカードからコマンドに対するレスポンスを受信するまで暗号鍵ＳＫ’を保持する。一方、ＩＣカードのコマンド解析部４２１は、受信機から受信した前記コマンドＣＯＭ（Ｒ）の内容を解析し、乱数Ｒを取り出して暗号鍵生成部４２２に出力する。暗号鍵生成部はＳＫ記憶部４２２に記憶されているセッション鍵ＳＫとコマンド解析部から入力された乱数Ｒから暗号鍵ＳＫ’を生成して暗号化部４０７に出力する。さらに、暗号鍵生成部４２２は、前記生成したＳＫ’をＳＫ記憶部４２０に出力し、ＳＫを更新する。ここで、受信機の暗号鍵生成部３２３と、ＩＣカードの暗号鍵生成部４２２との暗号鍵生成アルゴリズムは等しい。暗号化部４０７は、受信機から入力された前記コマンドに対するレスポンスデータＲＥＳをＳＫ’を鍵として暗号化したＥｎｃ（ＳＫ’，ＲＥＳ）を出力し、入出力部４０１から受信機へ送信する。受信機は、入出力部３０１がコマンドに対するレスポンスとしてＩＣカードからＥｎｃ（ＳＫ’，ＲＥＳ）を受信すると、復号部３０８は前記保持していたＳＫ’を鍵として復号し、レスポンスデータＲＥＳを出力する。

【００４４】次に、受信機がＩＣカードに対してコマンドを送信し、続けて、暗号化した通信データをＩＣカードへ送信する処理について説明する。たとえば、番組視聴の課金に関する情報や著作権に関する情報等、不正に取得されると悪用される恐れのある情報をＩＣカード内に蓄えたい場合、受信機はその旨を通知するコマンドをＩＣカードに送信し、さらにそれらの情報を暗号化して送信する。

【００４５】受信機の暗号鍵生成部３２３、及びＩＣカードの暗号鍵生成部４２２がＳＫ’を生成し、それぞれＳＫ記憶部３２０及び４２０にＳＫ’を記憶してＳＫを更新するところまでは、前述のＩＣカードからの通信データを受信機が受信する処理についての説明と同様である。しかし、受信機の暗号鍵生成部３２３はＳＫ’を暗号化部３２４へ、ＩＣカードの暗号鍵生成部４２２はＳＫ’を復号部４２３へ出力する。受信機の暗号化部３２４は通信データＤＡＴＡをＳＫ’を鍵として暗号化したＥｎｃ（ＳＫ’，ＤＡＴＡ）を出力し、入出力部３０１からＩＣカードへ送信する。ＩＣカードは、入出力部４０１が受信機からＥｎｃ（ＳＫ’，ＤＡＴＡ）を受信すると、復号部４２３は前記保持していたＳＫ’を鍵として復号し、ＤＡＴＡを出力する。

【００４６】このように、受信機からＩＣカードへ発信するコマンド毎に乱数を生成し、ＩＣカードへコマンドと共に乱数を送信し、受信機及びＩＣカードで共通のアルゴリズムを用いて暗号鍵ＳＫ’を生成すると、コマンドの度にリフレッシュされる鍵を用いた暗号化が可能となり、セッション鍵ＳＫを暗号鍵として用いた暗号通信と比較して、さらにセキュリティの高い暗号通信を実現できる。また、暗号鍵生成の度にＳＫが更新されるため、たとえ乱数Ｒが以前に用いた値と等しくなったとしても、ＳＫ’は異なり、乱数Ｒの盗聴によるＳＫ’の割り出しは困難という利点がある。

【００４７】なお、必ずしも全てのコマンドに対して乱数を生成して暗号鍵ＳＫ’を毎回更新しなくてもよい。一定のコマンド生成回数もしくは一定の時間が経過したタイミングで乱数を生成するようにしてもよい。受信機からのコマンドに乱数が含まれない場合は、受信機及びＩＣカードの復号部及び暗号化部は、既に保持しているＳＫ’を用いて暗号通信してもよい。この場合、受信機及びＩＣカードにおいて、暗号鍵生成処理及びＳＫ更新処理を省略することができる。

【００４８】図１２は、受信装置の認証処理の後に受信機がスクランブル鍵Ｋｓを保持するまでの処理を時系列に示すタイミングチャート図である。放送局は予め、受信機メーカー毎に、１つのＩＣカードに対する認証情報C_{ij}をｎ×ｍ個保持している。受信機は予め、自メーカーのデバイス鍵Kd_iをｎ個保持している。ＩＣカードは予め、ＩＣカード固有鍵KIC_jをｍ個と、個別鍵Ｋｍを保持している。

【００４９】まず、受信装置認証フェーズについて説明する。受信機は、放送局から送出されたC_{ij}を受信すると、ＩＣカードに送信する。ＩＣカードはC_{ij}を受信すると、フィルタリング処理を行ってC'_{ij}を生成し、受信機に送信する。受信機はC'_{ij}を受信すると、Kd_iを用いて復号し、KIC_jを取得する。受信機とＩＣカードは、共有できたKIC_jを用いて相互認証を行い、セッション鍵ＳＫを取得する。

【００５０】次に、視聴契約更新フェーズについて説明する。視聴契約更新フェーズでは、ＩＣカードが、ＥＭＭからスクランブル鍵Ｋｓを復号するために必要となるワーク鍵Ｋｗを取得する。受信機は、放送局から送出された自受信装置宛てのＥＭＭを受信すると、ＩＣカードに送信する。ＩＣカードはＥＭＭを受信すると、個別鍵Ｋｍを用いてＥＭＭを復号し、ワーク鍵Ｋｗを取得する。

【００５１】次に、番組視聴フェーズについて説明する。番組視聴フェーズでは、ＩＣカードが、ＥＣＭから番組をデスクランブルするために必要となるスクランブル鍵Ｋｓを取得し、受信機に送信する。受信機は、放送局から送出されたＥＣＭを受信すると、ＩＣカードに送信する。この時、乱数ＲもＩＣカードに送信し、さらに、受信装置認証フェーズで得たＳＫとＲから暗号鍵ＳＫ’を生成する。ＩＣカードはＥＣＭを受信すると、ワーク鍵Ｋｗを用いてＥＣＭを復号し、Ｋｓを取得する。さらに、受信した乱数Ｒと、受信装置認証フェーズで得たＳＫとから暗号鍵ＳＫ’を生成し、Ｋｓを暗号化して受信機に送信する。受信機は受信した暗号化済みＫｓを受信すると、前記生成したＳＫ’を用いて復号し、Ｋｓを得る。以降、受信機は、放送局から送出されるＥＣＭを受信する度に同様の処理を行い、Ｋｓを取得する。その際、値の異なる乱数（Ｒ’，Ｒ’’，．．．）が用いられ、また、暗号鍵ＳＫ’も毎回異なるもの（ＳＫ’，ＳＫ’’，．．．）に更新されていく。

【００５２】なお、視聴契約更新フェーズは、一度実行されると、視聴契約を更新するまでは実行されなくてもよい。これまでに説明のあった受信装置が受信する放送波の放送形態は、地上放送、衛生放送、有線放送（ＣＡＴＶ）のいずれであってもよい。また、その他の放送形態であってもよい。

【００５３】

【発明の効果】以上の説明から明らかなように、本発明の限定受信装置認証方法及び限定受信装置では、放送波を使って受信装置認証情報を受信装置に送ることにより、ＩＣカードが予め保持しているＩＣカード固有鍵KIC_jを受信機が保持できるため、受信機とＩＣカードとで予めグローバルシークレットを共有せずとも共有情報を安全に共有することができる。前記共有情報を用いて、認証処理を行うことにより、認証処理の都度更新されるセッション鍵ＳＫを生成することができ、ＳＫを用いてスクランブル鍵Ｋｓを暗号化して、Ｋｓを安全に受信機に送ることが可能となる。さらに、受信機からＩＣカードへ対するコマンド毎に乱数を送信することにより、受信機及びＩＣカードがそれぞれ前記乱数とＳＫとからコマンド毎に異なる暗号鍵ＳＫ’を生成して共有することができ、コマンドに対するＩＣカードからのレスポンスデータや受信装置本体からＩＣカードへの通信データを暗号化して、安全なデータの受け渡しが可能となる。

【００５４】また、ＩＣカード固有鍵を１つのＩＣカードにおいて複数保持できる方式であるため、相互認証時の通信データから最初のＩＣカード固有鍵を割り出されたとしても、別のＩＣカード固有鍵に対応する受信装置認証情報を放送局から送出することにより、Ｋｓを不正に取得されることを防ぐことができる。また、ＩＣカード固有鍵は全てのＩＣカードで異なっているため、万が一、あるＩＣカードのＩＣカード固有鍵の値が全て割り出されたとしても、限定受信システム運用への影響は軽微である。

【図面の簡単な説明】

【図１】従来の限定受信システムの送信側の構成を示すブロック図

【図２】従来の限定受信装置の構成を示すブロック図

【図３】本発明のデバイス鍵及びＩＣカード固有鍵をそれぞれ受信機及びＩＣカードに格納する手順の一例を示す図

【図４】本発明の受信装置認証情報を生成する方法を示すブロック図

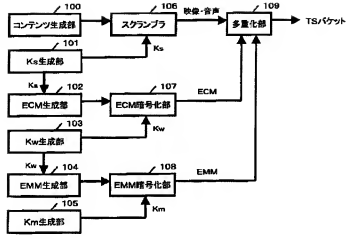
【図５】本発明の限定受信装置認証方法を用いた限定受信システムにおける送信側の構成を示すブロック図

【図６】本発明の限定受信装置が認証処理を行う方法を示すブロック図

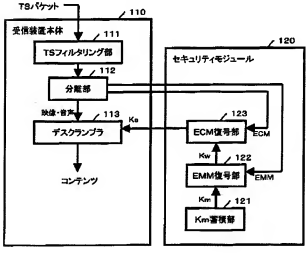
【図７】従来の相互認証方法の一例を示すブロック図

【図８】本発明の限定受信装置がＩＣカードに受信装置認証情報記憶部を具備した場合の認証処理を行う方法を示すブロック図
【図９】本発明の限定受信装置認証方法の手順を示すフローチャート
【図１０】本発明の限定受信装置が受信装置本体に受信装置認証情報フィルタリング部を具備した場合の認証方法を示すブロック図
【図１１】本発明の限定受信装置がコマンド毎に乱数を生成してＩＣカードに送信し、暗号鍵を生成して暗号通信を行う方法を示すブロック図
【図１２】本発明の限定受信装置認証方法を用いた限定受信システムにおいて、受信装置の認証処理の後に受信機がスクランブル鍵Ｋｓを保持するまでの処理を時系列に示すタイミングチャート
【符号の説明】
１００　コンテンツ生成部
１０１　Ｋｓ生成部
１０２　ＥＣＭ生成部
１０３　Ｋｗ生成部
１０４　ＥＭＭ生成部
１０５　Ｋｍ生成部
１０６　スクランブラ
１０７　ＥＣＭ暗号化部
１０８　ＥＭＭ暗号化部
１０９　多重化部
１１０　受信装置本体
１１１　ＴＳフィルタリング部
１１２　分離部
１１３　デスクランブラ
１２０　セキュリティモジュール
１２１　Ｋｍ蓄積部
１２２　ＥＭＭ復号部
１２３　ＥＣＭ復号部
１３０　（C_{u}，ｉ，ｊ）生成部
１３１　多重化部
２００　放送局
２０１　鍵管理センタ
２０２　デバイス鍵生成部
２０３　デバイス鍵ＤＢ
２０４　ＩＣカード固有鍵生成部
２０５　ＩＣカード固有鍵ＤＢ
２０６　受信機メーカー
２０７　受信機
２０８　ＩＣカードメーカー
２０９　ＩＣカード
２１０　受信装置認証情報生成部
２１１　暗号化部
３００　受信機
３０１　入出力部
３０２　ＴＳフィルタリング部
３０３　分離部
３０４　メーカーＩＤ記憶部
３０５　デバイス鍵記憶部
３０６　認証情報復号部
３０７　認証処理部
３０８　復号部
３０９　受信装置認証情報フィルタリング部
３１０　相互認証部
３２０　ＳＫ記憶部
３２１　乱数生成部
３２２　コマンド生成部
３２３　暗号鍵生成部
３２４　暗号化部
４００　ＩＣカード
４０１　入出力部
４０２　メーカーＩＤ記憶部
４０３　カードＩＤ記憶部
４０４　受信装置認証情報フィルタリング部
４０５　ＩＣカード固有鍵記憶部
４０６　認証処理部
４０７　暗号化部
４０８　Ｋｍ蓄積部
４０９　ＥＭＭ復号部
４１０　ＥＣＭ復号部
４１１　受信装置認証情報記憶部
４１２　受信装置認証情報フィルタリング部
４１３　相互認証部
４２０　ＳＫ記憶部
４２１　コマンド解析部
４２２　暗号鍵生成部
４２３　復号部

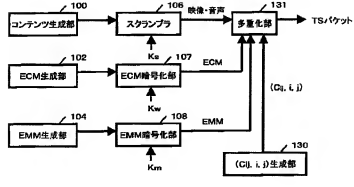
【図1】


100
コンテンツ生成部
106
スクランブラ
映像・音声
109
多重化部
TSパケット
101
Ks生成部
Ks
102
ECM生成部
107
ECM暗号化部
ECM
103
Kw生成部
Kw
104
EMM生成部
108
EMM暗号化部
EMM
105
Km生成部
Km

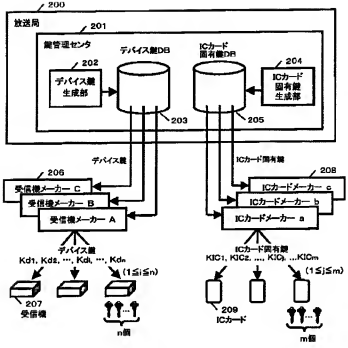
【図2】


TSパケット
110
受信装置本体
111
TSフィルタリング部
112
分離部
映像・音声
113
Ks
デスクランブラ
コンテンツ
120
セキュリティモジュール
123
ECM復号部
ECM
Kw
122
EMM復号部
EMM
Km
121
Km蓄積部

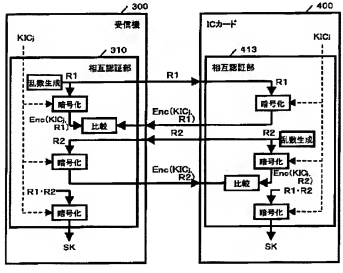
【図5】


100
コンテンツ生成部
106
スクランブラ
映像・音声
131
多重化部
TSパケット
Ks
102
ECM生成部
107
ECM暗号化部
ECM
(Ci, i, j)
Kw
104
EMM生成部
108
EMM暗号化部
EMM
130
(Ci), i, j)生成部
Km

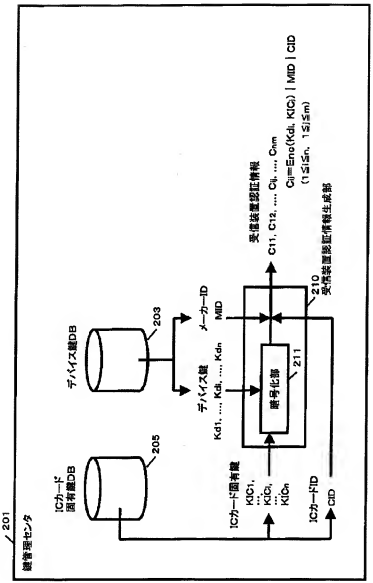
【図３】


200
放送局
201
鍵管理センタ
デバイス鍵DB
ICカード固有鍵DB
202
デバイス鍵生成部
204
ICカード固有鍵生成部
203
205
デバイス鍵
ICカード固有鍵
206
208
受信機メーカー C
受信機メーカー B
受信機メーカー A
ICカードメーカー c
ICカードメーカー b
ICカードメーカー a
デバイス鍵
Kd1, Kd2, ···, Kdi, ···, Kdn
(1≦i≦n)
ICカード固有鍵
KIC1, KIC2, ..., KICj, ...KICm
(1≦j≦m)
207
受信機
n個
209
ICカード
m個

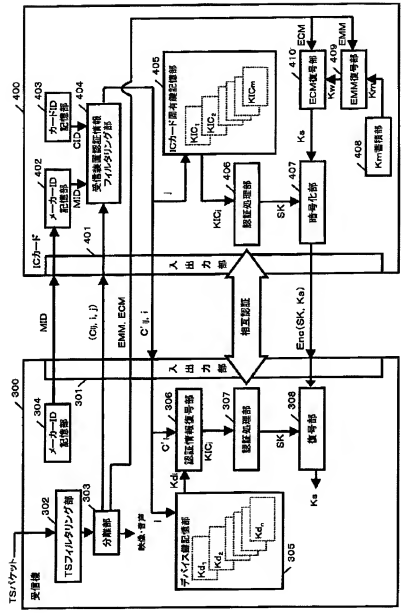
【図７】


300
受信機
KICi
310
相互認証部
乱数生成
R1
暗号化
Enc(KICi, R1)
比較
R2
暗号化
R1･R2
暗号化
SK
400
ICカード
KICi
413
相互認証部
R1
暗号化
R2
乱数生成
暗号化
Enc(KICi, R2)
比較
R1･R2
暗号化
SK

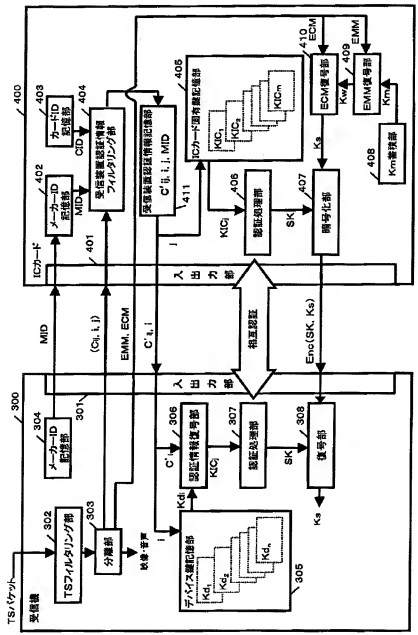
【図4】


201
鍵管理センタ
ICカード
固有鍵DB
205
デバイス鍵DB
203
ICカード固有鍵
KIC1,
KIC2,
KICn
デバイス鍵
Kd1, ... Kdn
メーカーID
MID
暗号化部
211
210
受信装置認証情報生成部
受信装置認証情報
C11, C12, ... C1n, ... Cm
Cij=Enc(Kdi, KICj) | MID | CID
(1≦i≦n, 1≦j≦m)
ICカードID
CID

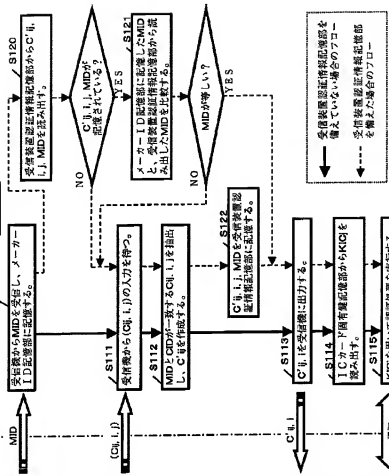
【図6】


TSパケット
受信機
TSフィルタリング部
分離部
映像・音声
メーカーID記憶部
メーカーID
MID
CID
ICカード
メーカーID記憶部
カードID記憶部
受信機固有識別情報フィルタリング部
ICカード固有鍵記憶部
認証処理部
暗号化部
ECM復号部
EMM復号部
Km復号部
デバイス鍵記憶部
認証情報復号部
認証処理部
復号部
入出力部
相互認証
MID
(CIDi, i, j)
EMM, ECM
C'i, i
Enc(SK, Ks)
EMM
ECM
Kd1
Kd2
Kdn
KIC1
KIC2
KICn
SK
Ks
Km
C'i
i
j

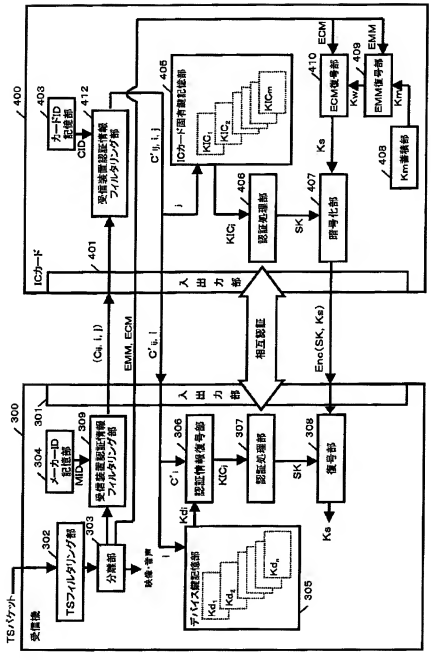
【図８】


400
ICカード
403
カードID記憶部
CID
404
受信装置認証情報フィルタリング部
MID
402
メーカーID記憶部
401
受信装置認証情報記憶部
C'ti, i, i, MID
405
ICカード固有鍵記憶部
KIC1
KIC2
KICn
411
406
認証処理部
KICi
SK
407
暗号化部
Ks
410
ECM
ECM復号部
Kw
409
EMM
EMM復号部
Km
408
Km蓄積部
入出力部
MID
(Ci, i, i)
EMM, ECM
C'i, i
相互認証
Enc(SK, Ks)
300
304
メーカーID記憶部
301
306
C'
認証情報復号部
Kdi
307
認証処理部
SK
308
復号部
Ks
TSパケット
受信機
302
TSフィルタリング部
303
分離部
映像・音声
ディバイス鍵記憶部
Kd1
Kd2
Kdn
305

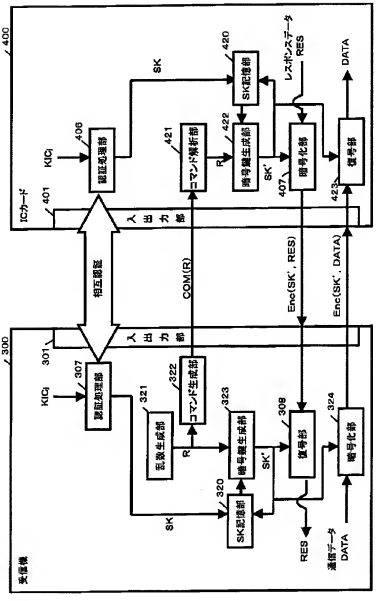
【図9】


受信機
ICカード
MID
(Cij, i, j)
C'ij, i, j
認証
S100
ICカードにメーカーIDを出力する。
S101
放送波を分離し、(Cij, i, j)を受信したらICカードに出力する。
S102
ICカードからC'ij, i, jの入力を待つ。
S103
デバイス識別部からKidを読み出し、C'ijを復元して、Kidを復元する。
S104
Kidを用いて認証処理を実行する。
S110
受信機からMIDを受け、メーカーID記憶部に記憶する。
S111
受信機から(Cij, i, j)の入力を待つ。
S112
MIDとCIDが一致するC'ij, i, jを指示し、C'ijを作成する。
S113
C'ij, i, jを受信機に出力する。
S114
ICカード識別情報記憶部からKidを読み出す。
S115
Kidを用いて認証処理を実行する。
S120
受信装置認証情報記憶部からC'ij, i, j, MIDを読み出す。
NO
C'ij, i, j, MIDが記憶されている？
YES
S121
メーカーID記憶部に記憶したMIDと、受信装置認証情報記憶部から読み出したMIDを比較する。
NO
MIDが等しい？
YES
S122
C'ij, i, j, MIDを受信装置認証情報記憶部に記憶する。
受信装置認証情報記憶部を備えていない場合のフロー
受信装置認証情報記憶部を備えた場合のフロー

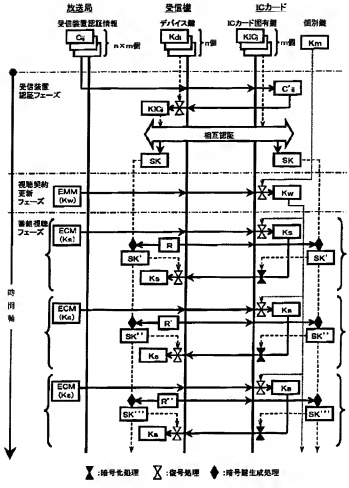
【図１０】


400
ICカード
401
403
カードID記憶部
CID
412
受信装置認証情報フィルタリング部
C'(j, i, j)
405
ICカード固有識別情報部
KIC1
KIC2
KICm
j
406
認証処理部
KICj
407
SK
暗号化部
Ka
410
ECM復号部
Kw
409
EMM復号部
Km
408
Km蓄積部
ECM
EMM
入出力部
相互認証
Enc(SK, Ka)
(Ca, i, j)
EMM, ECM
C'(j, i, j)
300
301
受信機
TSパケット
302
TSフィルタリング部
303
分離部
映像・音声
304
カードID記憶部
CID
309
受信装置認証情報フィルタリング部
MID
C'j
306
認証情報復号部
KICj
307
認証処理部
SK
308
復号部
Ka
Kdj
305
デバイス固有識別情報部
Kd1
Kd2
Kdn

【図１１】


400
ICカード
401
KIDi
406
認証処理部
SK
420
SK記憶部
レスポンスデータ
RES
DATA
421
コマンド解析部
R
422
暗号鍵生成部
SK'
407
暗号化部
423
復号部
入出力部
相互認証
COM(R)
Enc(SK', RES)
Enc(SK', DATA)
300
301
307
認証処理部
KIDi
321
乱数生成部
322
コマンド生成部
323
暗号鍵生成部
308
復号部
324
暗号化部
320
SK記憶部
SK
RES
通信データ
DATA
装置機

【図１２】



フロントページの続き

(72)発明者　黒岩　渉
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(72)発明者　熊崎　洋児
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(72)発明者　西條　猛
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(72)発明者　井上　哲也
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　松尾　隆史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　村上　弘規
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　布田　裕一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考) 5C064 CA14 CB01 CB08 CC01 CC04
5J104 AA07 AA16 EA04 EA22 EA24
KA02 KA04 NA03 NA35 NA36
NA37 NA41 NA42 PA05

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成19年11月29日(2007.11.29)

【公開番号】特開2002-152194(P2002-152194A)
【公開日】平成14年5月24日(2002.5.24)
【出願番号】特願2000-344384(P2000-344384)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｈ　1/00　(2006.01)
Ｈ０４Ｈ　1/02　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｈ　1/00　Ｆ
Ｈ０４Ｈ　1/02　Ｅ
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｎ　7/167　Ｚ

【手続補正書】
【提出日】平成19年10月15日(2007.10.15)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムの限定受信装置であって、
前記セキュリティモジュールとのデータ入出力を行う入出力手段と、
１つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、
前記１つ以上の限定受信装置固有情報のうちーの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記入出力手段を介して入力される暗号化されている情報を復号する復号手段と、
前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段と
を具備することを特徴とする限定受信装置。
【請求項２】
限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、
前記メーカーＩＤを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段と
を具備することを特徴とする請求項１に記載の限定受信装置。
【請求項３】
放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムのセキュリティモジ

ュールであって、
前記限定受信装置とのデータ入出力を行う入出力手段と、
セキュリティモジュールを一意に識別するセキュリティモジュールＩＤを記憶するセキュリティモジュールＩＤ記憶手段と、
前記セキュリティモジュールＩＤを参照して、前記限定受信装置から前記入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、
１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、
前記１つ以上のセキュリティモジュール固有情報のうちーのセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と
を具備することを特徴とするセキュリティモジュール。
【請求項４】
前記セキュリティモジュールはＩＣカードであり、前記セキュリティモジュールＩＤはカードＩＤである、請求項３記載のセキュリティモジュール。
【請求項５】
前記限定受信装置から前記入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段をさらに具備し、
前記フィルタリング手段は、前記メーカーＩＤと前記カードＩＤとを参照して、前記限定受信装置から前記入出力手段を介して入力される受信装置認証情報をフィルタリングすることを特徴とする請求項４に記載のセキュリティモジュール。
【請求項６】
前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項３から請求項５のいずれか一項に記載のセキュリティモジュール。
【請求項７】
放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、
前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、
限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、
１つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、
前記１つ以上の限定受信装置固有情報のうちーの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、
前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、
前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、
セキュリティモジュールを一意に識別するセキュリティモジュールＩＤを記憶するセキュリティモジュールＩＤ記憶手段と、
前記限定受信装置から前記第二入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、
前記メーカーＩＤと前記セキュリティモジュールＩＤとを参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、
１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、
前記１つ以上のセキュリティモジュール固有情報のうちーのセキュリティモジュール固

有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と

を具備することを特徴とする限定受信システム。

【請求項８】

前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項７に記載の限定受信システム。

【請求項９】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、

前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、

限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、

前記メーカーＩＤを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段と、

１つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、

前記１つ以上の限定受信装置固有情報のうち一の限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、

前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、

セキュリティモジュールを一意に識別するセキュリティモジュールＩＤを記憶するセキュリティモジュールＩＤ記憶手段と、

前記セキュリティモジュールＩＤを参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記１つ以上のセキュリティモジュール固有情報のうち一のセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と

を具備することを特徴とする限定受信システム。

【請求項１０】

前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項９に記載の限定受信システム。

【請求項１１】

セキュリティモジュールが装着されている限定受信装置の認証方法であって、

前記限定受信装置が、

受信した放送波に含まれる受信装置認証情報を分離するステップと、

自受信装置宛の受信装置認証情報だけを取り出すフィルタリング処理ステップと、

前記受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成するステップと、

前記限定受信装置と前記セキュリティモジュールとが、

前記限定受信装置と前記セキュリティモジュールとが共有した前記セキュリティモジュール固有情報を用いて認証処理を行うステップを有することを特徴とする限定受信装置認証方法。

【請求項１２】

前記受信装置認証情報は、前記限定受信装置が１つ以上保持する限定受信装置固有情報のいずれか１つを鍵として、前記セキュリティモジュールが１つ以上保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報のいずれか１つを暗号化することにより生成される情報と、限定受信装置のメーカーを識別するメーカーＩＤと、セキュリティモジュールを識別するセキュリティモジュールＩＤとを含み、

受信装置認証情報の生成に用いた限定受信装置固有情報及びセキュリティモジュール固有情報を特定するためのインデックス情報に組み合わせて、放送局設備から放送波を用いて送出されることを特徴とする、請求項１１に記載の限定受信装置認証方法。

【請求項１３】

前記フィルタリング処理は、前記メーカーＩＤと前記セキュリティモジュールが記憶しているセキュリティモジュールＩＤとが一致する受信装置認証情報を自受信装置宛の受信装置認証情報として選択することを特徴とする請求項１１及び請求項１２のいずれか一項に記載の限定受信装置認証方法。

【請求項１４】

前記限定受信装置で生成される前記共有情報は、前記限定受信装置固有情報を鍵として、前記受信装置認証情報に含まれる情報を復号することにより復元されることを特徴とする、請求項１１から請求項１３のいずれか一項に記載の限定受信装置認証方法。

【請求項１５】

前記フィルタリング処理は、前記限定受信装置において、当該限定受信装置が記憶しているメーカーＩＤと一致する受信装置認証情報を選択し、前記セキュリティモジュールにおいて、当該セキュリティモジュールが記憶しているセキュリティモジュールＩＤと一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項１１から請求項１４のいずれか一項に記載の限定受信装置認証方法。

【請求項１６】

前記セキュリティモジュールは、当該セキュリティモジュールが前記限定受信装置に装着された後に前記限定受信装置から入力されるメーカーＩＤを記憶するステップを有することを特徴とする、請求項１１から請求項１４のいずれか一項に記載の限定受信装置認証方法。

【請求項１７】

前記フィルタリング処理は、前記セキュリティモジュールにおいて、前記記憶されたメーカーＩＤと前記セキュリティモジュールが記憶しているセキュリティモジュールＩＤとが一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項１６に記載の限定受信装置認証方法。

【請求項１８】

前記セキュリティモジュールは、フィルタリング処理により抽出した受信装置認証情報を記憶するステップを有し、

前記セキュリティモジュールが前記限定受信装置に装着された後に前記限定受信装置から入力されるメーカーＩＤが前記記憶している受信装置認証情報に含まれるメーカーＩＤと等しい場合は、前記記憶している受信装置認証情報を前記限定受信装置に出力し、

前記限定受信装置は、前記セキュリティモジュールから被された前記受信装置認証情報を基に前記共有情報を生成することを特徴とする、請求項１５から請求項１７のいずれか一項に記載の限定受信装置認証方法。

【請求項１９】

前記認証処理手段が出力した前記セキュリティモジュールとの共有値を記憶する記憶手段と、

乱数を出力する乱数生成手段と、

前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて前記セキュリティモジュールから前記入出力手段を介して入力され

る情報を復号する復号手段と
をさらに具備することを特徴とする、請求項１及び請求項２のいずれか一項に記載の限定受信装置。
【請求項２０】
前記暗号鍵を用いて前記セキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備することを特徴とする、請求項１９に記載の限定受信装置。
【請求項２１】
前記認証処理手段が出力した前記限定受信装置との共有値を記憶する記憶手段と、
前記記憶している共有値と前記限定受信装置から前記入出力手段を介して入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、
前記暗号鍵を用いて前記限定受信装置へ出力する情報を暗号化する暗号化手段と
をさらに具備することを特徴とする、請求項３から請求項６のいずれか一項に記載のセキュリティモジュール。
【請求項２２】
前記暗号鍵を用いて前記限定受信装置から前記入出力手段を介して入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項２１に記載のセキュリティモジュール。
【請求項２３】
放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、
前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、
限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、
１つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、
前記１つ以上の限定受信装置固有情報のうち一の限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、
前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段と、
前記認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と、
乱数を出力する乱数生成手段と、
前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、
前記暗号鍵を用いて前記セキュリティモジュールから前記第一入出力手段を介して入力される情報を復号する復号手段とを具備し、
前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、
セキュリティモジュールを一意に識別するセキュリティモジュールＩＤを記憶するセキュリティモジュールＩＤ記憶手段と、
前記限定受信装置から前記第二入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカーＩＤを記憶するメーカーＩＤ記憶手段と、
前記メーカーＩＤと前記セキュリティモジュールＩＤとを参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、
１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、
前記１つ以上のセキュリティモジュール固有情報のうち一のセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値

を出力する認証処理手段と、
前記認証処理手段が出力した限定受信装置との共有値を記憶する記憶手段と、
前記記憶している共有値と前記限定受信装置から前記第二入出力手段を介して入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、
前記暗号鍵を用いて前記限定受信装置へ出力する情報を暗号化する暗号化手段とを具備することを特徴とする限定受信システム。
【請求項２４】
前記限定受信装置は、前記暗号鍵を用いて前記セキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備し、
前記セキュリティモジュールは、前記暗号鍵を用いて前記限定受信装置から前記第二入出力手段を介して入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項２３に記載の限定受信システム。
【請求項２５】
セキュリティモジュールが装着されている限定受信装置と前記セキュリティモジュール間の暗号通信方法であって、
前記限定受信装置は、前記セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップを有し、
前記セキュリティモジュールは、前記限定受信装置との認証処理によって生成した共有値を記憶するステップを有し、
前記限定受信装置及び前記セキュリティモジュールは、それぞれが記憶した共有値を鍵として用いて暗号通信を行うことを特徴とする、暗号通信方法。
【請求項２６】
セキュリティモジュールが装着されている限定受信装置と前記セキュリティモジュール間の暗号通信方法であって、
前記限定受信装置は、前記セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップと、
乱数を生成するステップと、
前記乱数を前記セキュリティモジュールに出力するステップと、
前記記憶したセキュリティモジュールとの共有値と前記乱数とを用いて暗号鍵を生成するステップとを有し、
前記セキュリティモジュールは、前記限定受信装置との認証処理によって生成した共有値を記憶するステップと、
前記記憶した限定受信装置との共有値と前記限定受信装置から入力された乱数とを用いて暗号鍵を生成するステップと、
前記暗号鍵を前記限定受信装置との共有値として記憶するステップとを有し、
前記限定受信装置及び前記セキュリティモジュールは、それぞれが生成した暗号鍵を用いて暗号通信を行うことを特徴とする、暗号通信方法。
【請求項２７】
前記限定受信装置は、前記生成した暗号鍵を前記セキュリティモジュールとの新しい共有値として記憶するステップをさらに有し、
前記セキュリティモジュールは、前記生成した暗号鍵を前記限定受信装置との新しい共有値として記憶するステップをさらに有することを特徴とする、請求項２６に記載の暗号通信方法。
【請求項２８】
前記限定受信装置から前記セキュリティモジュールへのコマンド送信をトリガーとして、前記限定受信装置が前記乱数を生成することを特徴とする、請求項２６及び請求項２７のいずれか一項に記載の暗号通信方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の名称

【補正方法】変更
【補正の内容】
【発明の名称】限定受信システムの限定受信装置及びセキュリティモジュール、限定受信システム、限定受信装置認証方法及び暗号通信方法
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
【発明の属する技術分野】
本発明は、視聴契約を必要とする放送システム（限定受信システム）に関し、特に、限定受信システムを構成する限定受信装置とセキュリティモジュールとの間で安全に暗号通信を行う技術に関する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正の内容】
【０００５】
多重化部で多重化された信号はＴＳパケット（Transport Stream Packet）に変換されて送出される。一方、番組を視聴する受信側の構成は、図２に示すように、限定受信装置（受信機）１１０と、受信機に装着されるＩＣカード等のセキュリティモジュール１２０とを備えており、受信機は選局されたＴＳパケットだけを取り込むＴＳフィルタリング部１１１と、多重されている信号を分離する分離部１１２と、スクランブルされたコンテンツを復号化するデスクランブラ１１３とを具備し、また、セキュリティモジュールは、Ｋｍを保持するＫｍ蓄積部１２１と、Ｋｍを用いてＥＭＭを復号するＥＭＭ復号部１２２と、Ｋｗを用いてＥＣＭを復号するＥＣＭ復号部１２３とを具備している。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正の内容】
【００１０】
【発明が解決しようとする課題】
これまでの説明から明らかなように、限定受信装置とセキュリティモジュールとの間で安全な暗号通信を行うためには、限定受信装置とセキュリティモジュールとが、共有情報を安全に共有することが重要である。予め共有情報をグローバルシークレットとして限定受信装置とセキュリティモジュールとに格納した場合、セッション毎に相互認証を行うことにより、セッション毎に異なる安全なセッション鍵を共有することが可能である。しかし、この場合、悪意を持つ者が限定受信装置とセキュリティモジュールとの間で通信される相互認証用データ（チャレンジ・レスポンス等）を不正取得して暗号解読を試み、万が一、共有情報の割り出しに成功すると、セッション鍵の割り出しが可能となり、その結果、スクランブル鍵Ｋｓや、視聴契約情報、課金情報といった限定受信装置とセキュリティモジュールとの間で通信されるデータが不正に取得されてしまう。また、割り出された共有情報は、全ての受信装置において共通であるため、限定受信システム運用に与えるダメージは非常に重大である。システム運用を回復するための対処として、新しい共有情報を暗号化して格納した記憶メディアを全視聴者に配布して受信機及びセキュリティモジュールの共有情報を更新する方法が考えられるが、これは膨大なコストの発生を伴うと予想され、非現実的である。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
また、限定受信装置とＩＣカード等のセキュリティモジュールの製造は、それぞれ複数の異なるメーカーが担当するのが一般的である。予め共有情報を限定受信装置及びセキュリティモジュールに格納しておく場合、全てのメーカー製の限定受信装置と、全てのメーカー製のセキュリティモジュールとの組み合わせにおいて相互認証を正しく行うためには、メーカーを問わず、全ての限定受信装置及びセキュリティモジュールで等しい共有情報を共有する必要がある。この場合、ある１つのメーカーにおける機密情報管理レベルが低く、メーカー内部から共有情報の漏洩が発生してしまうと、他のメーカー製の限定受信装置及びセキュリティモジュールにもその影響が波及し、限定受信システムの運用に致命的なダメージを及ぼすことになる。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
本発明は、こうした問題点を解決するものであり、限定受信装置とセキュリティモジュールとで予め共通の共有情報を持たずとも、セッション鍵生成等で用いる共有情報を安全に共有することができる限定受信システムの限定受信装置及びセキュリティモジュール、限定受信システム、限定受信装置の認証方法、及び、暗号通信方法を提供することを目的とする。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】
【課題を解決するための手段】
この課題を解決するために本発明は、限定受信装置にセキュリティモジュールが装着される構成を取る限定受信システムにおいて、限定受信装置は限定受信装置を製造するメーカーを識別するＩＤを記憶するメーカーＩＤ記憶手段と、１つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、前記１つ以上の限定受信装置固有情報のうち一の限定受信装置固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールはセキュリティモジュールを一意に識別するセキュリティモジュールＩＤを記憶するセキュリティモジュールＩＤ記憶手段と、前記メーカーＩＤと前記セキュリティモジュールＩＤとを参照して受信装置認証情報をフィルタリングするフィルタリング手段と、１つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、前記１つ以上のセキュリティモジュール固有情報のうち一のセキュリティモジュール固有情報を入力として限定受信装置との認証処理を行う認証処理手段を備えることを特徴とする。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更

【補正の内容】
【００１４】
また、放送局設備において受信装置認証情報を生成し、受信装置認証情報を放送局から放送波を用いて送出し、限定受信装置は受信した受信装置認証情報からメーカーＩＤとセキュリティモジュールＩＤを検索キーとして自受信装置宛の受信装置認証情報だけをフィルタリングし、フィルタリングした受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成して、限定受信装置とセキュリティモジュールは前記共有情報を用いて認証処理を行う。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
また、受信装置認証情報は、限定受信装置が保持する限定受信装置固有情報を鍵としてセキュリティモジュールが保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報を暗号化することにより生成される情報と、限定受信装置のメーカーを識別するメーカーＩＤと、セキュリティモジュールを識別するセキュリティモジュールＩＤとから構成される。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
以上により、限定受信装置とセキュリティモジュールとでセキュリティモジュール固有情報を共有し、その共有情報を基に、限定受信装置とセキュリティモジュールとの間の暗号通信に用いるセッション鍵を生成する。また、限定受信装置は乱数生成手段と、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備え、セキュリティモジュールは、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備える。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
また、限定受信装置は乱数を生成してセキュリティモジュールに出力すると共に、セッション鍵記憶手段から読み出したセッション鍵と前記乱数とから暗号鍵を生成する。さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。セキュリティモジュールは、限定受信装置から入力した乱数と、セッション鍵記憶手段から読み出したセッション鍵とから暗号鍵を生成する、さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
以上により、限定受信装置とセキュリティモジュールとで共通の暗号鍵を共有し、暗号

通信を行う。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
【発明の実施の形態】
本発明の実施の形態について、図を用いて説明する。なお、以降では、限定受信装置を受信機、セキュリティモジュールをＩＣカード、限定受信装置固有情報をデバイス鍵、セキュリティモジュール固有情報をＩＣカード固有鍵と記述して説明する。